Aritmética modular

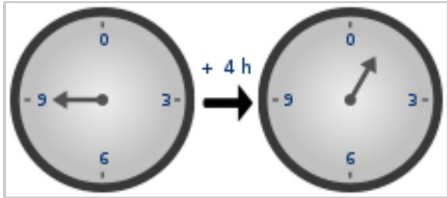
Origem: Wikipédia, a enciclopédia livre.

Em matemática, **aritmética modular** (chamada também de **aritmética do relógio**) é um sistema de aritmética para inteiros, onde os números "voltam pra trás" quando atingem um certo valor, o **módulo**.

O matemático suiço Euler foi o pioneiro na abordagem de congruência por volta de 1750, quando ele explicitamente introduziu a ideia de congruência módulo um número natural *N*.[1]

A aritmética modular foi desenvolvida posteriormente por Carl Friedrich Gauss em seu livro *Disquisitiones Arithmeticae*, publicado em 1801.

Um uso familiar da aritmética modular é no relógio de ponteiro, no qual o dia é divido em dois períodos de 12 horas cada. Se a hora é 7 horas agora, então daqui a 8 horas serão 3 horas. A adição usual sugere que o tempo futuro deveria ser 7 + 8 = 15, mas esta é a resposta errada por que o relógio "volta pra tràs" a cada 12 horas; não existe "15 horas" no relógio de ponteiro. Da mesma forma, se o relógio começa em 12:00(meio dia) e 21 horas passam, então a hora será 9:00 do dia seguinte, em vez de 33:00. Como o número de horas começa de novo depois que atinge 12, esta aritmética é chamada aritmética módulo 12. 12 é congruente não só a 12 mesmo, mas também a 0, assim a hora chamada "12:00" pode também ser chamada "0:00", pois 0 ≡ 12 mod 12.



O relógio usa aritmética módulo 12.

Índice

Relação de congruência

Aritmética modular pode ser tratada matematicamente introduzindo uma relação de congruência no conjunto dos inteiros que é compatível com as operações do anel dos inteiros: adição, subtração e multiplicação. Para um inteiro positivo *n*, dois inteiros *a* e *b* são ditos **congruêntes** (ou **côngruos**) **módulo** *n*, e escrevemos

$$a \equiv b \pmod{n},$$

quando a diferença deles $a - b$. é um inteiro múltiplo de *n*. O número *n* é chamado o **módulo** da congruência.

Por exemplo,

$$38 \equiv 2 \pmod{12}$$

pois 38 − 2 = 36, que é múltiplo de 12.

A mesma regra é vale para valores negativos:

$$-8 \equiv 7 \pmod{5}.$$
$$2 \equiv -3 \pmod{5}.$$
$$-3 \equiv -8 \pmod{5}.$$

Se a e b são ou os dois positivos ou os dois negativos, então $a \equiv b \pmod{n}$ pode ser visto como a afirmação de que a/n e b/n tem o mesmo resto. Por exemplo

$$38 \equiv 14 \pmod{12}$$

porque ambos $38/12$ e $14/12$ tem o mesmo resto 2. Observe que também tem-se $38 - 14 = 24$ um inteiro multiplo de 12, concordando com a definição inicial de relação de congruência.

Uma observação sobre a notação: Como é comum considerar várias relações de congruência com diferentes módulos ao mesmo tempo, o módulo é incorporado na notação. Mesmo a notação sendo ternária a relação de congruência para um módulo fixado é uma relação binária. Isto deve estar claro se a notação $a \equiv_n b$ for usada, em vez da notação tradicional.

As propriedades que fazem desta relação uma relação de congruência (com respeito à adição, subtração e multiplicação) são as seguintes.

Se

$$a_1 \equiv b_1 \pmod{n}$$

e

$$a_2 \equiv b_2 \pmod{n},$$

então:

- $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$
- $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$

Deve-se notar que as propriedades acima continuam válidas se expandirmos a teoria para incluir todos os números reais, mas a propriedade seguinte não vale necessariamente nesse contexto ampliado

- $a_1 a_2 \equiv b_1 b_2 \pmod{n}.$

Não se faz divisão em congruências, ao invés disso, faz-se uma multiplicação em ambos os membros por um número conveniente.

Pelo fato de todo número ter resto 0 na divisão por 1 não é interessante usarmos o módulo 1,pois para quaisquer a e b inteiros sempre teremos $a \equiv b \equiv 0 \mod 1$.

Anel de classes de congruência

Como qualquer relação de congruência, congruência módulo *n* é uma relação de equivalência, e as classes de equivalência do inteiro *a*, denotada por $\overline{a}_n$, é o conjunto $\{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$. Este conjunto, consistindo dos inteiros congruentes a *a* modulo *n*, é chamado a **classe de congruência** ou **classe de resíduos** ou simplesmente **resíduo** do inteiro *a*, modulo *n*. Quando o módulo *n* é conhecido pelo contexto, este **resíduo** também pode ser denotado por $[a]$.

O conjunto de todas as classes de congruência módulo *n* é denotado $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}/n$ (a notação alternativa $\mathbb{Z}_n$ não é recomendada por causa da possível confusão com o conjunto dos inteiros p-ádicos). E é definida por : $\mathbb{Z}/n\mathbb{Z} = \{\overline{a}_n | a \in \mathbb{Z}\}$.

Quando $n \neq 0$, $\mathbb{Z}/n\mathbb{Z}$ tem *n* elementos, e pode ser escrita como:

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}_n, \overline{1}_n, \overline{2}_n, \ldots, \overline{n-1}_n\right\}.$$

Quando *n* = 0, $\mathbb{Z}/n\mathbb{Z}$ não tem elementos não nulos; daí é isomorfo a $\mathbb{Z}$, pois $\overline{a}_0 = \{a\}$.

Podemos definir adição, subtração e multiplicação em $\mathbb{Z}/n\mathbb{Z}$ pelas seguintes regras:

- $\overline{a}_n + \overline{b}_n = \overline{(a+b)}_n$
- $\overline{a}_n - \overline{b}_n = \overline{(a-b)}_n$
- $\overline{a}_n \overline{b}_n = \overline{(ab)}_n$.

A verificação que esta é uma definição adequada usa as propriedades mencionadas antes.

Desta forma, $\mathbb{Z}/n\mathbb{Z}$ se torna um anel comutativo. Por exemplo, no anel $\mathbb{Z}/24\mathbb{Z}$, temos

$$\overline{12}_{24} + \overline{21}_{24} = \overline{9}_{24}$$

como na aritmética do relógio de ponteiro.

A notação $\mathbb{Z}/n\mathbb{Z}$ é usada, por que ele é anel quociente de $\mathbb{Z}$ pelo ideal $n\mathbb{Z}$ consistindo de todos os inteiros divisíveis por *n*, onde $0\mathbb{Z}$ é o conjunto unitário $\{0\}$. Assim $\mathbb{Z}/n\mathbb{Z}$ é um corpo quando $n\mathbb{Z}$ é um ideal máximal, ou seja, quando n é primo.

Em termos de grupos, a classe de resíduos $\overline{a}_n$ é a classe lateral de *a* no grupo quociente $\mathbb{Z}/n\mathbb{Z}$, um grupo cíclico.[2]

O conjunto $\mathbb{Z}/n\mathbb{Z}$ tem várias propriedades matemáticas importantes que são o fundamento de vários ramos da matemática.

Em vez de excluir o caso *n*=0, é mais útil incluir $\mathbb{Z}/0\mathbb{Z}$ (que, como mencionado antes, é isomorfo ao anel $\mathbb{Z}$ dos inteiros), por exemplo quando discutindo característica de um anel.

Restos

A noção de aritmética modular está relacionada com a de resto da divisão. A operação de achar o resto é algumas vezes chamada de operação módulo, nesse contexto escrevemos, por exemplo, 2 = 14 (mod 12). A diferença está no uso da congruência, indicado por "≡", e da igualdade indicado por "=". Igualdade implica especificamente o "resíduo comum", o menor inteiro não negativo membro de uma classe de equivalência. Quando estamos trabalhando com aritmética modular, cada classe de equivalência é geralmente representada pelo seu resíduo comum, por exemplo 38 ≡ 2 (mod 12), que pode ser encontrado usando

divisão longa. Segue disso que enquanto é correto dizer 38 ≡ 14 (mod 12) e 2 ≡ 14 (mod 12), é incorreto dizer 38 = 14 (mod 12) (com "=" no lugar de "≡").

A diferença é mais clara quando estamos dividindo um número negativo, por que neste caso os restos são negativos. Assim para expressar o resto devemos escrever −5 ≡ −17 (mod 12), em vez de 7 = −17 (mod 12), pois equivalência só pode ser considerada para resíduos com o mesmo sinal.

Em ciência da computação, o operador resto é normalmente indicado por "%" (e.g. in C, Java, Javascript, Perl e Python) ou "mod" (e.g. in Pascal, BASIC, SQL, Haskell), com exceções(e.g. Excel). Estes operadores são normalmente pronunciados como "mod", mas o que é efetivamente computado é um resto (pois em C++ são retornados números negativos se o primeiro argumento é negativo e em Python um número negativo é retornado se o segundo argumento é negativo). A função *modulo* em vez de *mod*, como em 38 ≡ 14 (modulo 12), é algumas vezes usada para indicar um resíduo comum em vez do resto (e.g. em Ruby).

Os parenteses às vezes não são escritos na expressão, por exemplo 38 ≡ 14 mod 12 ou 2 = 14 mod 12, ou são colocados em volta do divisor, por exemplo 38 ≡ 14 mod (12). Notações como 38(mod 12) também existem, mas são ambíguas sem um contexto.

Representação funcional da operação resto

A operação resto pode ser representada usando função piso. Se $b=a \pmod n$, onde $n>0$, então se o resto é b ele é dado por

$$b = a - \left\lfloor \frac{a}{n} \right\rfloor \times n,$$

onde $\left\lfloor \frac{a}{n} \right\rfloor$ é o maior inteiro menor ou igual a $\frac{a}{n}$, então

$$a \equiv b \pmod n \text{ e,}$$
$$0 \leq b < n.$$

Se em vez do resto b o intervalo $-n \leq b < 0$ é requirido, então

$$b = a - \left\lfloor \frac{a}{n} \right\rfloor \times n - n.$$

Sistema de resíduos

Cada classe de resíduo modulo n pode ser representada por um de seus membros, embora nós geralmente representemos cada classe residual pelo menor inteiro não negativo pertencente à classe (pois este é o próprio resto que resulta da divisão). Note que quaisquer dois membros de diferentes classes residuais módulo n são congruentes módulo n. Além disso cada inteiro pertence a uma e somente uma classe residual módulo n.[3]

O conjunto de inteiros {0, 1, 2, ..., *n* - 1} é chamado o **menor sistema de resíduos módulo *n*** . Qualquer outro conjunto de *n* inteiros, com nenhum par deles congruente módulo *n* é chamado um **sistema completo de resíduos módulo *n*** .

É claro que o menor sistema de resíduos é uma sistema completo de resíduos e que um sistema completo de resíduos é simplesmente um conjunto contendo precisamente um representante de cada classe de resíduo módulo *n*. O menor sistema de resíduos módulo 4 é {0, 1, 2, 3}. Alguns outros sistemas de resíduos módulo 4 são:

- {1,2,3,4}
- {13,14,15,16}
- {-2,-1,0,1}
- {-13,4,17,18}
- {-5,0,6,21}
- {27,32,37,42}

Alguns conjuntos que não são um sistema completo de resíduos módulo 4 são:

- {-5,0,6,22} pois 6 é congruente a 22 módulo 4.
- {5,15} pois um sistema completo de resíduos deve ter exatamente 4 elementos.

Sistemas reduzidos de resíduos

Qualquer conjunto com φ(*n*) inteiros que são primos com *n* e que são incongruentes entre si módulo *n*, onde φ(*n*) denota a Função totiente de Euler, é chamado um **sistema reduzido de resíduos módulo *n*** .

Referências

1. http://www.ams.org/samplings/feature-column/fcarc-eulers-formula
2. Arnaldo Garcia e Yves Lequain. Elementos de Álgebra - Rio de Janeiro, IMPA, 2002. 326 páginas (Projeto Euclides), ISBN 978-85-244-0190-9
3. José Plinio de Oliveira Santos - Introdução à Teoria dos Números - Rio de Janeiro, IMPA, 1998. 198 péginas (projeto Euclides), ISBN 978-85-244-0142-8

Categorias: Aritmética modular | Matemática | Matemática discreta